

## (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
14 June 2001 (14.06.2001)

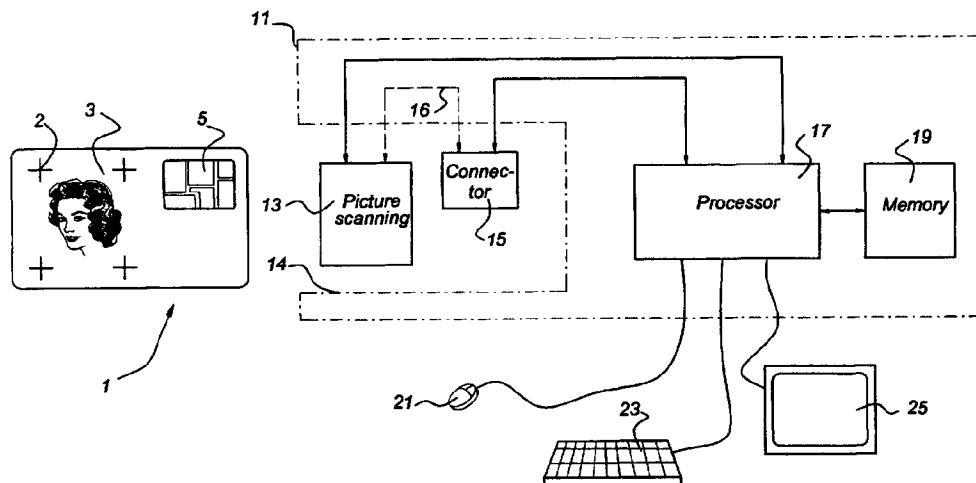
PCT

(10) International Publication Number  
**WO 01/43080 A1**

- (51) International Patent Classification<sup>7</sup>: **G07C 9/00**
- (21) International Application Number: PCT/NL99/00749
- (22) International Filing Date: 7 December 1999 (07.12.1999)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): **SUN MICROSYSTEMS INC.** [US/US]; San Antonio Road, MS PALI-521, Palo Alto, CA 94303 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **DE JONG, Eduard, Karel** [NL/NL]; Ankersmidplein 63, NL-1506 CK Zaan-dam (NL).
- (81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- Published:  
— With international search report.
- (74) Agent: **DE BRUIJN, Leendert, C.**; Nederlandsch Octrooibureau, Scheveningseweg 82, P.O. Box 29720, NL-2502 LS The Hague (NL).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE PHOTO CARRYING IDENTIFICATION DEVICE, AS WELL AS MEANS AND METHOD FOR AUTHENTICATING SUCH AN IDENTIFICATION DEVICE



(57) Abstract: Means and a method for authenticating a photographic image (3) on an identification device (1), the identification device (1) being provided with: a photographic image of a person (3) and a microprocessor (8), the microprocessor (8) having: a) a processor (7), b) a memory (9) connected to the processor (7) and having stored authentication data, and c) interface means (5) connected to the processor (7) for communicating with an external device, wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said photographic image (3), the method having the following steps: a') scanning the photographic image (3) and generating image data, b') analyzing these image data in accordance with a predetermined image analysis procedure to derive said hidden information, and c') carrying out the authentication of the photographic image (3) based on the hidden information and the authentication data.

**Secure photo carrying identification device, as well as means and method for authenticating such an identification device**

5

Field of the invention

The present invention relates to a photo carrying identification device, like passports, and (credit) cards used to identify persons, and thereafter authorize them to do a predetermined action, like entering a building, passing a boarder, carrying out an automatic debit transaction from an account, etc.

10

Background of the invention

The invention relates to the use of identification (ID) documents equipped with a picture of a document's holder, e.g., a driver's licence, or a plastic card having the size of a credit card, or a passport. In a common use of such an ID document, a human operator compares the picture on the document with the face of the document holder to assess entitlements sought by the document's holder based on credentials as defined by additional data in the document. A passport, for instance, gives access to a country based on nationality of the document's holder.

15

A problem encountered with such documents is that they are frequently copied with false credentials or a false picture.

A common solution to this problem is the application of physical tamper detection methods such a sealing foil covering both the picture and the document, often combined with special inspection tools, like polarized light, to probe the tamper detection method. However, the use of such inspection tools often requires a skilled operator.

20

Another possible solution, referred to in paragraph [0002] of EP-B1-0,539,439, to tampering with the picture attached to the ID document is in using smart cards provided with a microprocessor having a processor and a memory. The memory in the card chip stores a digital copy of the picture on the card. A terminal is provided to read the content of the memory of the chip card and to display the stored image on a monitor to an operator. Then, the operator compares the displayed image on the monitor with the

25

30

face of the actual card holder. This solution may even obviate the need to attach the picture on the card itself. However, this solution requires costly display equipment which, amongst other reasons, has made this solution unsuitable in particular areas of industry which offers great potential to the use of smart cards, such as public transit systems where ID smart cards are sought as efficient improvement of traditional discount passes.

A further problem encountered in ID systems is in protecting the privacy of the individual using the ID document. Especially in case such an ID document is realized as an electronically readable smart card protection may be required from uncontrolled and/or unapproved collection of data identifying the individual and his or her use of the smart card.

To protect the privacy of the card holder, cryptographic techniques, e.g., blind signatures, may be applied to the process of reading ID and credential data from the smart card. However, the use of pictures stored in a card memory and read by a terminal for display on a monitor to an operator in principle defeats such cryptographic privacy protection. In such a case, the terminal is not only able to collect uniquely and strongly identifying data about individuals, i.e. their pictures, but also the nature of this data poses an additional threat in which, for instance, the individual may be compromised through digital image manipulation techniques.

US-A-5,748,763, column 58, line 24, to column 62, line 45, describes a method and an arrangement for enhancing the security of credit and debit cards. The arrangement disclosed has a computer arranged for receiving a digital image of the card holder. After having analyzed the digital image the computer generates a snowy image which is generally orthogonal to the digital image and adds this to the digital image to render an amended, unique image. The intended effect is to "texturize" the original digital image. It is not necessary that the snowy image itself is invisible to a person looking at the image. However, the image of the card holder may not be obscured by the snowy image. The amended, unique image is printed on the card. Moreover, the unique information is also stored in a central accounting network.

In a steganographic embodiment the snowy image is such that it is hidden in the photographic image of the person on the card. More detailed information as to steganography can be found in US Patent 5,613,004 and the references cited in this document. For the sake of the present invention steganography will be understood to relate

WO 01/43080

PCT/NL99/00749

3

to any method of obscuring information that is otherwise in plain sight. The information is hidden in another medium. It is used as an alternative to encryption. E.g., spreadsheets or graphics files could contain a text message invisible to an unaware person. People unaware of the hidden information will not recognize the presence of

5 steganographically hidden information even if the information is in plain view.

In US-A-5,748,763, referred to above, a scanner is provided to scan the card when the card holder wishes to use his card for a predetermined transaction, e.g., automatic payment from his account to pay for a product. The scanner is connected to the central accounting network. By means of a secure communication protocol the

10 image of the card scanned by the scanner is transmitted to the central network. The central network is arranged to receive the transmitted information and to authenticate the validity of the image on the card.

Additional security to the known system may be provided by requesting the card holder to input a PIN during the scanning process. Moreover, additional security is provided by letting a third party, during the scanning process, check whether or not the

15 person trying to carry out a transaction with the card is the person who's photo is on the card.

A disadvantage of the system and method disclosed by US-A-5,748,763 is that it is only to operate when a central network is provided having stored all unique images

20 of all participating cards.

### Summary of the invention

A first object of the invention is to provide a photo carrying identification device

25 that obviates the need for such a central network.

Therefore the invention provides an identification device provided with:

- a photographic image of a person and
- a microprocessor,

the microprocessor comprising:

- 30
- a processor,
  - a memory connected to the processor and comprising authentication data, and
  - interface means connected to the processor for communicating with an external device;

wherein the photographic image comprises steganographically hidden information, the content of which together with the authentication data allows authentication of the photographic image.

Thus, the invention provides an identification device which are provided with a microprocessor, comprising the authentication data necessary to authenticate the photographic image on the identification device. In other words, the key to authenticate the photographic image is in the identification device itself instead of in a central network.

Such an identification device may be, for instance, a passport or a plastic identification card, like a smart card.

In one embodiment of the invention the processor is arranged to carry out at least part of the authentication. To that effect the processor will carry out a program preferably stored in the memory of the microprocessor.

The authentication data stored in the memory of the microprocessor may be a part of the photographic image on the identification device. However, it may also be data related to the photographic image. For instance, it may be related to grey level, intensity distribution, or image entropy of the photographic image.

A second object of the invention is to provide a terminal, which is arranged to communicate with the identification device of the invention to allow carrying out the authentication process required.

In a first embodiment the invention therefore provides a terminal arranged to communicate with an identification device, the identification device being provided with:

- a photographic image of a person and
- a microprocessor,

the microprocessor comprising:

- a processor,
- a memory connected to the processor and comprising authentication data, and
- interface means connected to the processor for communicating with a terminal,

wherein the photographic image comprises steganographically hidden information, the content of which together with the authentication data allows authentication of the photographic image,

the terminal being provided with:

- a picture scanner to scan the photographic image and to generate image data,

- a terminal interface allowing communication with the processor of the identification device, and
  - an image processor arranged
  - to receive the image data,
  - 5 ➤ to analyze these image data in accordance with a predetermined image analysis procedure to derive the hidden information,
  - to receive the authentication data from the memory, and
  - to carry out at least part of the authentication of the photographic image based on the authentication data and the hidden information.

10 In this first embodiment, the authentication of the photographic image is either partly or entirely carried out by the image processor in the terminal.

The steps necessary to carry out said authentication will, in practice, be stored in a terminal memory. In an embodiment of the invention, the way in which these steps are carried out depends on the authentication data received from the memory of the

15 identification device. In such an embodiment, the authentication carried out by the terminal will depend on data received from the identification device itself. This makes it impossible to predict the actual authentication steps carried out by the terminal, which enhances the security.

However, the security can also be enhanced in an alternative embodiment in

20 which the processor of the identification device itself carries out at least part of the authentication of the photographic image. Therefore, the invention also provides a second embodiment of the terminal. This second embodiment terminal is arranged to communicate with an identification device, the identification device being provided with:

- 25
- a photographic image of a person and
  - a microprocessor,  
the microprocessor comprising:
    - a processor,
    - a memory connected to the processor and comprising authentication data, and
    - 30 ➤ interface means connected to the processor for communicating with a terminal,
- wherein the photographic image comprises steganographically hidden information, the content of which together with the authentication data allows authentication of the photographic image,

WO 01/43080

PCT/NL99/00749

6

the processor being arranged to carry out at least part of the authentication of the photographic image,

the terminal being provided with:

- a picture scanner to scan the photographic image and to generate image data,
- 5 • a terminal interface allowing communication with the processor of the identification device, and
- an image processor arranged
  - to receive the image data,
  - to analyze these image data in accordance with a predetermined image analysis
  - 10 procedure to derive the hidden information, and
  - to transmit at least the hidden information to the processor to allow the processor to carry out the at least part of the authentication of the photographic image.

Moreover, the invention relates to a method for authenticating a photographic image on an identification device, the identification device being provided with:

- 15 • a photographic image of a person and
- a microprocessor,  
the microprocessor comprising:
  - a processor,
  - a memory connected to the processor and comprising authentication data, and
  - 20 ➤ interface means connected to the processor for communicating with an external device,

wherein the photographic image comprises steganographically hidden information, the content of which together with the authentication data allows authentication of the photographic image,

25 the method comprising the following steps:

- scanning the photographic image and generating image data,
- analyzing these image data in accordance with a predetermined image analysis procedure to derive the hidden information, and
- carrying out the authentication of the photographic image based on the hidden
- 30 information and the authentication data.

Finally, the invention relates to data carriers provided with a computer program and to computer programs as such for such a method.

Hereinafter, the present invention will be illustrated with reference to some drawings which are intended to illustrate the invention and not to limit its scope.

#### Brief description of the drawings

5

Figure 1 is a schematic drawing of the system according to the invention showing a smart card and a terminal;

figure 2 shows the functional units of the microprocessor of the smart card in a schematic way;

10 figure 3 schematically shows how information can be hidden in a photographic image;

figure 4 shows a flow diagram of the method according to the invention.

#### Detailed description of the embodiments

15

Figure 1 shows a smart card 1 provided with a photographic image 3 of the card holder. The smart card 1 is provided with an interface 5 shown to be made of metallic pads. However, the interface 5 may have any other form, e.g., an antenna hidden within the smart card 1 allowing for contactless communication with an external device.

20 As shown in figure 2, the interface 5 is connected to a card processor 7 which is also connected to a card memory 9.

Returning now to figure 1, the smart card 1 is, preferably, provided with one or more orientation signs 2 assisting a scanner during scanning the photographic image 3, as will be explained hereinafter.

25 It is observed that figure 1 shows a smart card 1 but that the invention is equally applicable for other types of documents having a photographic image of the document holder and a processor arranged to communicate with an external device.

The smart card 1 may be inserted into and removed from an opening 14 in a terminal 11. The terminal 11 is provided with a picture scanner 13 and a connector 15.

30 The picture scanner 13 is arranged such that it may scan the photographic image 3 either during insertion of the smart card 1 into the opening 14 or after the smart card 1 has been inserted entirely in opening 14.



The connector 15 will contact the interface 5 of the smart card 1 when the smart card 1 has been inserted entirely in the opening 14. Of course, when interface 5 is designed in another form, e.g. an antenna, the connector 15 is to be replaced by another type of interface arranged to communicate with interface 5.

5       The picture scanner 13 is connected to a processor 17 which is also connected to the connector 15 and to a memory 19.

Figure 1 also shows some input means, like a mouse 21, and a keyboard 23, allowing an operator to input data to the processor 17. A monitor 25 connected to the processor 17 is provided to allow the processor to display necessary information to the operator. Of course, any other kind of display means may be provided instead of or in  
10       addition to monitor 25.

In an alternative embodiment of the terminal shown in figure 1, the processor 17 is provided as a processing unit within the picture scanner 13. Then, the picture scanner 13 is directly connected to connector 15 (or any other interface) by a direct link indicated with reference sign 16.  
15       

Figure 3 schematically shows that the photographic image 3 is provided with additional information 4. The additional information 4 is added to the photographic image 3 such that it is invisible to the human eye. Moreover, the additional information 4 may have such small dimensions that it is virtually impossible to be detected by automatic scanners if they do not know where to look for the additional information. The additional information 4 is added to the photographic image 3 by using steganographic techniques which are known to persons skilled in the art.  
20       

It is observed that, in figure 3, the additional information 4 is shown on such an enlarged scale that it is visible but in practice it will not be visible to the human eye. Moreover, in a preferred embodiment, the individual dots of information 4 are distributed over the entire image 3 to make it more difficult to find them.  
25       

The additional information 4 may have no relation at all to the content of the photographic image 3. However, the photographic image 3 before being printed on the smart card 1 may be preprocessed in such a way that the additional information 4 is calculated in dependence on the content of the photographic image 3 such that the  
30       degree to which it is hidden in the photographic image 3 is as best as possible.

In accordance with the present invention, the card memory 9 is provided with authentication data. The content of this authentication data, together with the hidden information 4 allows authentication of the photographic image 3.

In its simplest form, the authentication data has a one to one relation to the hidden  
5 information 4. However, the hidden information 4 may be present within the photographic image 3 in cryptographically processed form, e.g., it may be provided with a cryptographic signature such that the validity of the hidden information 4 can only be checked by an apparatus knowing the key to the cryptographic signature. Such a key is, then, stored in the card memory 9.

10 The hidden information 4 is such that it can be recognized by digitization of the photographic image 3 even if it is incomplete or otherwise impaired. The hidden information may have the form of a digital watermark.

Checking the validity of the hidden information may be based on any kind of calculation using both the hidden information 4 and the authentication data in the card  
15 memory 9.

As shown in figure 4, in order to allow for authentication, the card holder has to insert his or her smart card 1 into the opening 14 of the terminal 11. During insertion or after completing the insertion, the picture scanner 13 scans the photographic image 3, while interfaces 5 and 15 may communicate with one another. The orientation signs 2  
20 may assist the picture scanner 13 in detecting where to search for the hidden information 4. The picture scanner 13 processes the photographic image 3 and generates image data which is sent to the processor 17, step 30.

The processor 17 digitally processes the received image data, as well as the authentication data stored in the card memory 9 in accordance with a predetermined  
25 program. In accordance with the predetermined program, which is preferably stored in memory 19, the processor 17 separates the hidden information 4 from the photographic image 3, step 32, and uses the hidden information 4 to establish the authenticity of the photographic image 3, step 34.

The authentication data received from the smart card 1 may be protected with any  
30 cryptographic means known to persons skilled in the art. Additionally, the data may be provided with a digital signature.

The authentication process carried out by the processor 17 may depend on the authentication data received from the smart card 1 in such a way that for different

authentication data a different authentication process is carried out. This further enhances security.

In an alternative embodiment, instead of the processor 17 in the terminal 11, the card processor 7 is arranged to carry out the authentication process. To that end, it  
5 receives the hidden information 4 by means of the terminal 11.

However, since the card processor 7 and its memory 9 will only have a limited capacity, in practice, it will be preferred that both the processor 17 of the terminal 11 and the card processor 7 carry out part of the authentication process. The card processor 7 may, for instance, perform a final authentication step of the authentication process.

10 In a further embodiment the card memory 9 may be provided with credential data, i.e., data indicating predetermined actions the card holder is allowed to do, e.g., entering a building or an area, debitting an account, etc. In that case, the card processor 7 is, preferably, arranged to transmit these credential data to the processor 17 only when its own part of the authentication process has been carried out successfully. Thus,  
15 by receiving the credential data the processor 17 is informed that the authentication steps carried out by card processor 7 did not find any problems. When it does not receive the credential data the processor 17 knows that the authentication process has been unsuccessful.

To further enhance the security, the authentication data stored in card memory 9  
20 may be related to one or more specific or general characteristics of the image 3 itself, like grey level, intensity distribution or image entropy. These parameters will be derived by the picture scanner 13 and transmitted to the processor 17. These parameters may be used by the processor 17 during the authentication process. However, in order to further enhance security, these parameters may be passed through the processor 17 to  
25 the card processor 7 which uses one or more of these parameters during carrying out its authentication steps.

Instead of the picture scanner 13 establishing the value of one or more of these parameters, these parameters may be digitally stored in the photographic image 3. The digitized value of these parameters may have been printed after being encoded. Before  
30 these digitized values of these parameters are added to the photographic image 3 they may be encoded.

In the embodiment described above, the terminal 11 is shown to include a memory 19. As is evident to persons skilled in the art memory 19 may comprise any

WO 01/43080

PCT/NL99/00749

11

kind of memory type like RAM, ROM, EPROM, EEPROM, etc. or any combination thereof. For the purpose of the present invention the memory 19 need not necessarily be physically located within the terminal 11.

Moreover, the processor 17 is shown to be one block. However, if preferred, the  
5 processor 17 may be implemented as several subprocessors communicating with one another each dedicated to perform a predetermined task. Preferably, the processor 17 is (or the subprocessors are) implemented as a computer with suitable software. However, if desired, they may be implemented as dedicated digital circuits.

The method in accordance with the present invention is preferably implemented  
10 by suitable software. This software may be distributed by data carriers like CDROM's or through the Internet or any other data communication medium.

WO 01/43080

PCT/NL99/00749

12

## Claims

1. Identification device (1) provided with:
- a photographic image of a person (3) and
- 5     • a microprocessor (8),  
the microprocessor (8) comprising:
- a processor (7),
  - a memory (9) connected to the processor (7) and comprising authentication data, and
- 10     ➤ interface means (5) connected to said processor (7) for communicating with an external device;
- wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said photographic image (3).
- 15
2. Identification device (1) according to claim 1, wherein said identification device (1) is one of the following set of items: passport and plastic identification card.
3. Identification device (1) according to claim 1 or 2, wherein said processor (7) is
- 20 arranged to carry out at least part of said authentication.
4. Identification device (1) according to claim 1, 2 or 3, wherein said hidden information is provided with a cryptographic signature.
- 25 5. Identification device (1) according to any of the preceding claims, wherein said authentication data is at least partly related to a feature of the photographic image (3).
6. Identification device (1) according to any of the preceding claims, wherein said hidden information is related to a feature of the photographic image (3).
- 30 7. Identification device (1) according to claim 5 or 6, wherein said feature is at least one of the following set of features: gray level, intensity distribution, and image entropy.

8. A terminal (11) arranged to communicate with an identification device (1), said identification device (1) being provided with:

- a photographic image of a person (3) and
- 5   • a microprocessor (8),  
the microprocessor (8) comprising:
  - a processor (7),
  - a memory (9) connected to the processor (7) and comprising authentication data, and
  - 10   ➤ interface means (5) connected to said processor (7) for communicating with a terminal (11),

wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said photographic image (3),

15 said terminal being provided with:

- a picture scanner (13) to scan the photographic image (3) and to generate image data,
- a terminal interface (15) allowing communication with said processor (7) of the identification device (5), and
- 20   • an image processor (17) arranged
  - to receive said image data,
  - to analyze these image data in accordance with a predetermined image analysis procedure to derive said hidden information,
  - to receive said authentication data from said memory (9), and
  - 25   ➤ to carry out at least part of said authentication of said photographic image (3) based on said authentication data and said hidden information.

9. A terminal according to claim 8, wherein said authentication comprises a set of predetermined steps stored in a terminal memory (19), the way in which said steps are  
30 carried out depending on said authentication data received from said memory (9) of said identification device (1).

10. A terminal (11) arranged to communicate with an identification device (1), said identification device (1) being provided with:

- a photographic image of a person (3) and
- a microprocessor (8),

5 the microprocessor (8) comprising:

- a processor (7),
- a memory (9) connected to the processor (7) and comprising authentication data, and
- interface means (5) connected to said processor (7) for communicating with a

10 terminal (11),

wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said photographic image (3),

said processor (7) being arranged to carry out at least part of said authentication of said

15 photographic image (3),

said terminal being provided with:

- a picture scanner (13) to scan the photographic image (3) and to generate image data,
- a terminal interface (15) allowing communication with said processor (7) of the

20 identification device (5), and

- an image processor (17) arranged

- to receive said image data,
- to analyze these image data in accordance with a predetermined image analysis procedure to derive said hidden information, and

25 ➤ to transmit at least said hidden information to said processor (7) to allow said processor (7) to carry out said at least part of said authentication of said photographic image (3).

11. A terminal according to claim 8, 9 or 10, wherein said terminal has an opening  
30 (14) for receiving said identification device (1), both said picture scanner (13) and said terminal interface (15) being located within said opening (14).

12. A terminal according to any of the claims 8 through 11, wherein said image processor (17) is integrated within said picture scanner (13).

13. A method for authenticating a photographic image (3) on an identification device (1), said identification device (1) being provided with:

- a photographic image of a person (3) and
- a microprocessor (8),  
the microprocessor (8) comprising:
  - a processor (7),
  - 10 ➤ a memory (9) connected to the processor (7) and comprising authentication data, and
  - interface means (5) connected to said processor (7) for communicating with an external device,

wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said photographic image (3),

said method comprising the following steps:

- scanning the photographic image (3) and generating image data,
- analyzing these image data in accordance with a predetermined image analysis procedure to derive said hidden information, and
- 20 • carrying out said authentication of said photographic image (3) based on said hidden information and said authentication data.

14. A data carrier provided with a computer readable program for a method for authenticating a photographic image (3) on an identification device (1), said identification device (1) being provided with:

- a photographic image of a person (3) and
- a microprocessor (8),  
the microprocessor (8) comprising:
  - 30 ➤ a processor (7),
  - a memory (9) connected to the processor (7) and comprising authentication data, and



- interface means (5) connected to said processor (7) for communicating with an external device,

wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said

5 photographic image (3),

said method comprising the following steps:

- scanning the photographic image (3) and generating image data,
- analyzing these image data in accordance with a predetermined image analysis procedure to derive said hidden information, and
- 10 • carrying out said authentication of said photographic image (3) based on said hidden information and said authentication data.

15 15. A computer program product for a method for authenticating a photographic image (3) on an identification device (1), said identification device (1) being provided with:

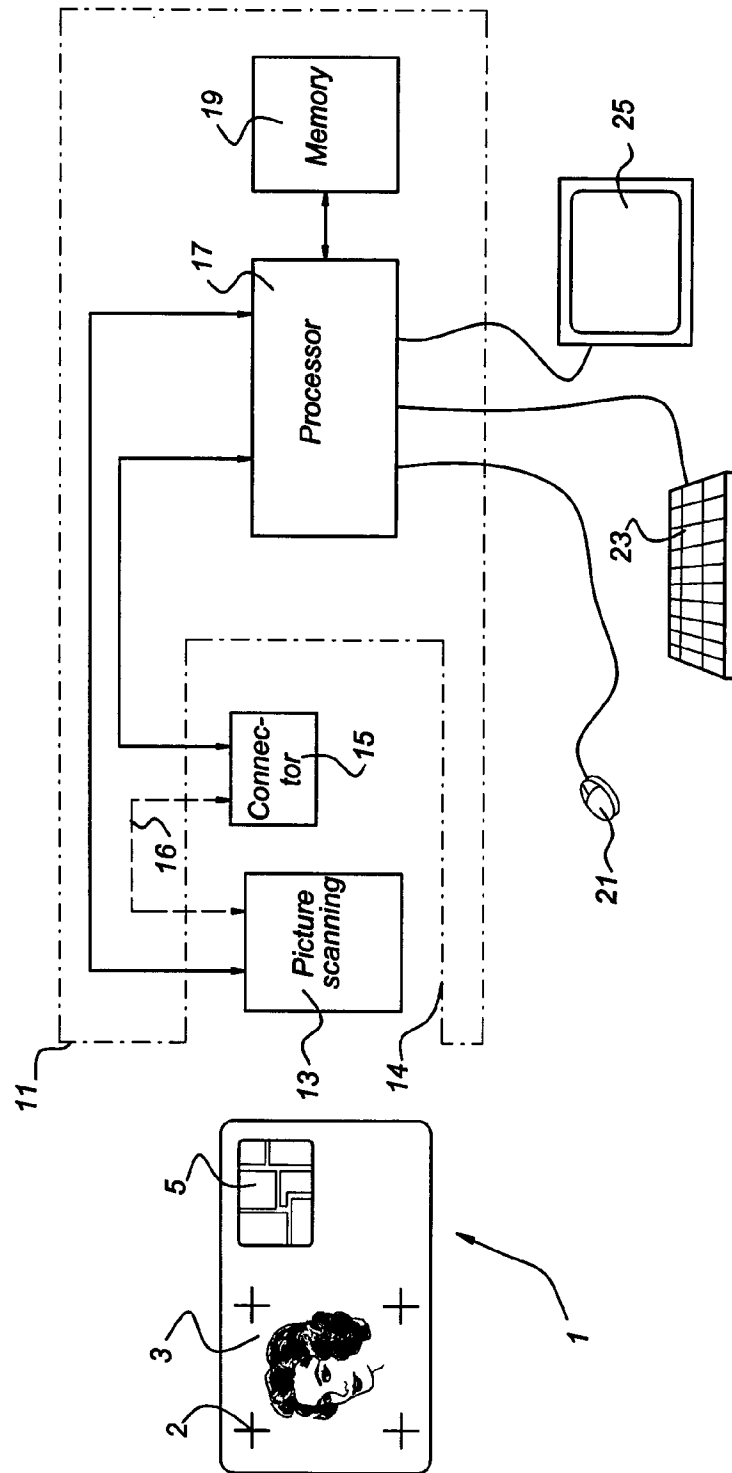
- a photographic image of a person (3) and
- a microprocessor (8),  
the microprocessor (8) comprising:
  - a processor (7),
  - 20 ➤ a memory (9) connected to the processor (7) and comprising authentication data, and
  - interface means (5) connected to said processor (7) for communicating with an external device,

25 wherein said photographic image (3) comprises steganographically hidden information, the content of which together with said authentication data allows authentication of said photographic image (3),

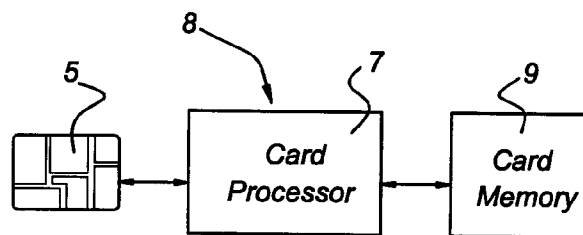
said method comprising the following steps:

- scanning the photographic image (3) and generating image data,
- analyzing these image data in accordance with a predetermined image analysis procedure to derive said hidden information, and
- 30 • carrying out said authentication of said photographic image (3) based on said hidden information and said authentication data.

Fig 1

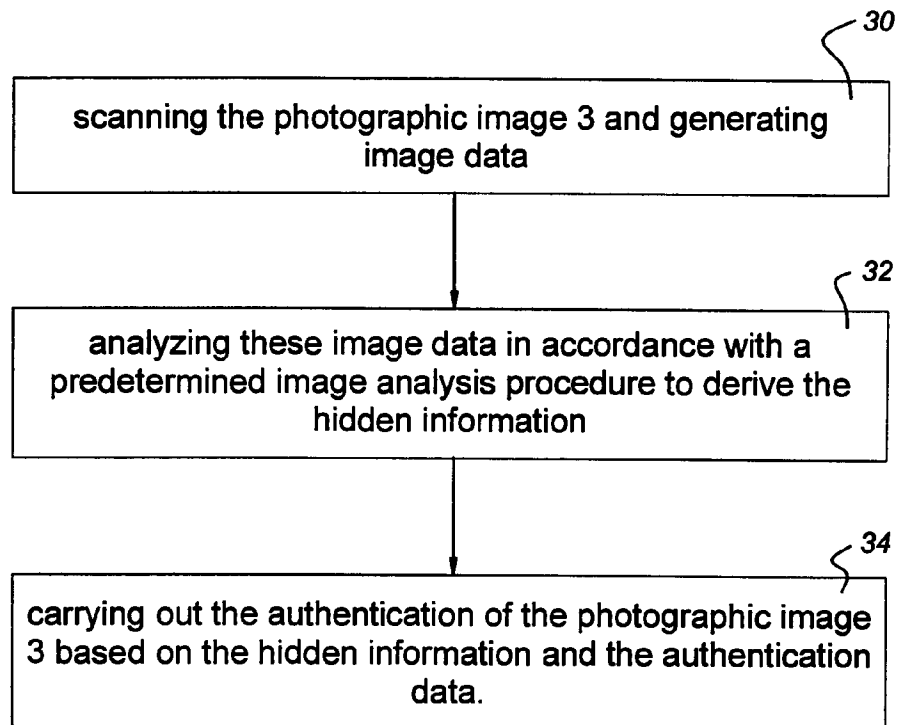


*Fig 2*



*Fig 3*



*Fig 4*

## INTERNATIONAL SEARCH REPORT

Intern. Appl. No.

PCT/NL 99/00749

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07C G07F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 776 153 A (ORDICAM RECH ET DEV) 17 September 1999 (1999-09-17) the whole document	1-6,8-15
Y	US 5 832 119 A (RHOADS GEOFFREY B) 3 November 1998 (1998-11-03) abstract column 58, line 55 -column 64, line 52 figures 22-24,28	1-6,8-15
Y	EP 0 864 996 A (HITACHI LTD) 16 September 1998 (1998-09-16) abstract	3,10
A	column 4, line 57 -column 5, line 27 figures 1,4	1,8
	--- -/--	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

## \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

10 August 2000

Date of mailing of the international search report

21/08/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Miltgen, E

## INTERNATIONAL SEARCH REPORT

Inter:      nal Application No

PCT/NL 99/00749

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MATSUI K ET AL: "VIDEO-STEGANOGRAPHY: HOW TO SECRETLY EMBED A SIGNATURE IN A PICTURE", IMA INTELLECTUAL PROPERTY PROJECT PROCEEDINGS, XX, XX, VOL. 1, NR. 1, PAGE(S) 187-206 XP000199949 the whole document ---	1-15
A	EP 0 674 295 A (GEMPLUS CARD INT) 27 September 1995 (1995-09-27) the whole document ---	1,2,8, 10,13
A	EP 0 581 317 A (INTERACTIVE HOME SYSTEMS) 2 February 1994 (1994-02-02) abstract page 2, line 27 - line 49 page 3, line 6 - line 51 figures 1,2 ---	1,8,10
A	US 4 921 278 A (SHIANG LU P ET AL) 1 May 1990 (1990-05-01) -----	

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/NL 99/00749

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2776153 A	17-09-1999	NONE	
US 5832119 A	03-11-1998	US 5841978 A	24-11-1998
		US 5636292 A	03-06-1997
		US 5768426 A	16-06-1998
		AU 6022396 A	29-11-1996
		CA 2218957 A	14-11-1996
		EP 0824821 A	25-02-1998
		WO 9636163 A	14-11-1996
		US 5862260 A	19-01-1999
		EP 0737387 A	16-10-1996
		JP 9509795 T	30-09-1997
		US 6064737 A	16-05-2000
		US 5841886 A	24-11-1998
		CA 2174413 A	26-05-1995
		EP 0959620 A	24-11-1999
		EP 0959621 A	24-11-1999
		EP 0987855 A	22-03-2000
		WO 9514289 A	26-05-1995
		US 5748763 A	05-05-1998
		US 5850481 A	15-12-1998
		US 6026193 A	15-02-2000
		US 5745604 A	28-04-1998
EP 0864996 A	16-09-1998	JP 10312459 A	24-11-1998
EP 0674295 A	27-09-1995	FR 2717931 A	29-09-1995
		US 5754675 A	19-05-1998
EP 0581317 A	02-02-1994	US 5721788 A	24-02-1998
		CA 2101673 A	01-02-1994
		JP 6343128 A	13-12-1994
		US 5930377 A	27-07-1999
		US 6072888 A	06-06-2000
		US 5809160 A	15-09-1998
US 4921278 A	01-05-1990	DE 3610445 A	06-11-1986
		JP 63158297 A	01-07-1988